

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro



(43) Internationales Veröffentlichungsdatum
25. März 2004 (25.03.2004)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2004/025437 A2

(51) Internationale Patentklassifikation⁷: **G06F 1/00**, H04L 29/06

(21) Internationales Aktenzeichen: PCT/EP2003/009040

(22) Internationales Anmeldedatum: 14. August 2003 (14.08.2003)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität: 102 39 062.2 26. August 2002 (26.08.2002) DE

(71) Anmelder (*für alle Bestimmungsstaaten mit Ausnahme von US*): SIEMENS AKTIENGESELLSCHAFT [DE/DE]; Wittelsbacherplatz 2, 80333 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder (*nur für US*): SCHMIDT, Andreas [DE/DE]; Neustadtring 48, 38114 Braunschweig (DE). TRAUBERG, Markus [DE/DE]; Valkeakoskistr. 6, 38159 Velchede (DE).

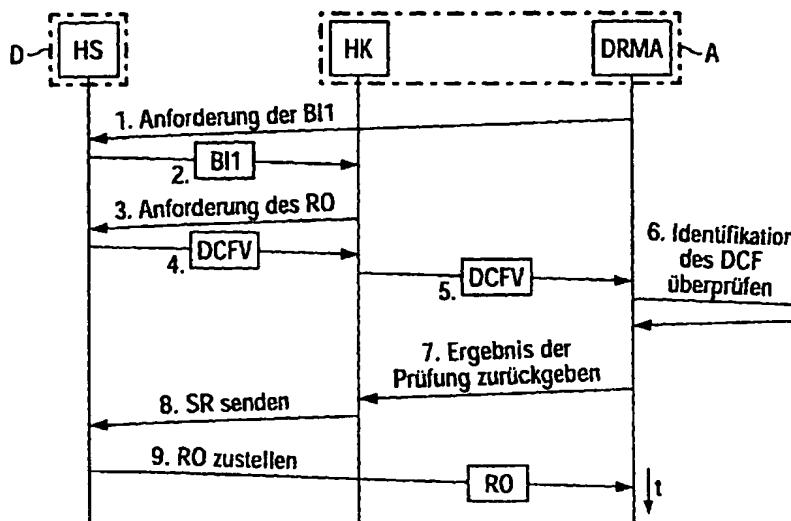
(74) Gemeinsamer Vertreter: SIEMENS AKTIENGESELLSCHAFT; Postfach 22 16 34, 80506 München (DE).

(81) Bestimmungsstaaten (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT,

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD FOR TRANSMITTING ENCRYPTED USER DATA OBJECTS

(54) Bezeichnung: VERFAHREN ZUM ÜBERTRAGEN VON VERSCHLÜSSELNEN NUTZDATEN-OBJEKTN



- 1 REQUEST BI1
- 3 REQUEST RO
- 6 VERIFY IDENTIFICATION OF DCF
- 7 RETURN RESULT OF VERIFICATION
- 8 TRANSMIT SR
- 9 SUPPLY RO

verify the compatibility of the desired rights object and the encrypted user data object provided in the telecommunications device and if said verification is successful, subsequently transmits the rights object (RO) to the telecommunications device (A).

[Fortsetzung auf der nächsten Seite]

WO 2004/025437 A2

(57) Abstract: The invention relates to a method for handling, in particular transmitting encrypted user data objects. According to said method, a data preparation component (D) of a data preparation system provides user data objects. The data preparation component first encrypts a user data object that has been prepared. It then determines a checksum of the encrypted user data object and creates a container data object (DCF), in which the encrypted user data object and the determined checksum are provided. The container data object is subsequently transmitted to a first telecommunications device (A). Preferably, in order to use the encrypted user data object, the data preparation component (D) transmits descriptive information (BI1) containing a description of the possible usage rights for the encrypted user data object to the telecommunications device (A). After the selection of a specific rights object (RO), the data preparation device first transmits a confirmation object (DCFV) to the telecommunications device in order to